DISTRIBUTED LEDGER TECHNOLOGIES FOR IoT: **LEARNINGS & OPERATOR ROLE**

GSMA Report

FEBRUARY 2020

TABLE OF CONTENTS

1. INTRODUCTION

Distributed ledger technology has become a topic of significant interest for use in the Internet of Things. The GSMA published the document 'Opportunities and Use Cases for Distributed Ledger Technologies in the IoT' in September 2018[1] and has since been working with mobile network operators to develop practical case studies and proofs of concept.

The technology platforms for distributed ledgers are proving their effectiveness for a wide range of applications, and meanwhile there is strong associated interest in how these can be incorporated into products and services offered by mobile network operators.

The intent of this document is to review the experiences from **the first public deployment of distributed ledgers applied to the IoT as a proof of concept by China Unicom and the GSMA**, and explore the new roles that mobile network operators can reasonably adopt with this relatively new technology. Of key interest is how mobile network operators can use distributed ledger technologies to open up new value generation opportunities for the IoT. Operators are starting to launch blockchain (i.e. distributed ledger) related products and services, for example Deutsche Telekom's T-Systems launch of a "Blockchain as a Service" marketplace which supports key applications such as multi-party supply chains.[2]

This document reflects on the following topics related to the China Unicom proof of concept:

- **Provide key learnings and thoughts about how operators can add value by using a distributed ledger technology (DLT) based solution to their customers**
- **Compare DLT solutions with non-DLT solutions supporting similar use cases**
- **Distil any particular learnings/ best practices that were obtained during the PoC so that other operators may not need to go through the same learning curve in future**
- **Identify potential areas of increased revenue opportunities for operators using or offering DLT for IoT services**

The document starts with an overview of the China Unicom proof of concept.

[1] See https://www.gsma.com/iot/resources/opportunities-distributed-ledger-in-iot/
[2] See https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-makes-blockchain-simple-for-business-customers-583652

2. INTRODUCTION TO THE CHINA UNICOM PROOF OF CONCEPT

The GSMA, China Unicom and industrial partners in China, defined and delivered a distributed ledger proof of concept during the first half of 2019.[3] The solution was aimed at showing how China Unicom could help an industrial partner address a business problem using a distributed ledger platform provided by China Unicom and its partners.

The specific end customer business problem being addressed related to the authenticity[4] of recorded information about rechargeable batteries used in electric vehicles (in this case used in buses). The lifetime, efficiency and value of rechargeable batteries is dependent on the number of charging cycles the battery has been through. Once a battery reaches the end of its usable life[5] for electric vehicles, and if it has been through a limited number of charging cycles, it can be resold for reuse in other applications, such as for reserve power storage for solar farms. If the battery has been through an excess number of charging cycles the materials should instead be recycled, with a consequential lower end of life valuation than if it could be resold for reuse in other applications. Currently there is no simple or trusted way to establish the number of charge cycles a rechargeable battery has been through and therefore resale/recycle value cannot be maximised. Instead, manufacturers or recyclers have to rely on costly electrical and chemical testing processes which evaluate the suitability of spent batteries for either reuse or materials recycling, as noted in the article "Lithium battery reusing and recycling: A circular economy insight".[6]

China Unicom are therefore looking to demonstrate how distributed ledger technologies, as used in cryptocurrencies such as bitcoin, can be applied to other business solutions.

Bitcoin has shown it is possible to secure transaction details (worth billions of dollars of value) through a distributed technical platform with no overall controlling party or system, therefore these solutions are robust. Although the China Unicom proof of concept does not involve payment processes, the technical features of distributed ledgers are applicable to securing transaction details relating to battery production, use and charge events. Of course the same records could be stored in conventional database platforms, but distributed ledgers offer the ability for all parties to hold replicas of the same immutable data, therefore adding to the confidence in the stored data.

> "The profit margin in the reuse of lithium-ion power batteries is unclear. Although data on batteries provided by lithium-ion power battery producers state that the batteries removed from new energy vehicles retain 70–80% valid energy and appear competitive in costs, there are still many challenges when energy storage is focused in the field of battery reuse[6]"

[4] Details of this are in the publication https://www.gsma.com/iot/resources/report-dlt-application-for-renewable-battery-value-evaluation-in-iot/

[4] i.e. being able to demonstrate data has not been tampered with

[5] i.e. maintaining sufficient charge to power the vehicle during its regular running period

[6] https://ncbi.nlm.nih.gov/pmc/articles/PMC6582158/

Within China, electric vehicles[7] are equipped to send reporting data to the Beijing Institute of Technology for various evaluations including transport planning. This reporting data includes battery charging information. This 'Big Data' collection platform contains in-life information about the charge cycles of batteries installed in vehicles, but does not contain other relevant information regarding the capacity of the battery / battery modules or the number of charge cycles the battery had been through prior to installation in the vehicle.

Whilst there is sufficient information available on batteries to make the reuse/recycle decision, it is contained within either a manufacturer 'silo' or a third party 'silo'. An independent proof of information authenticity is not available and the default position is that at 'end of life' batteries need to be tested to determine the remaining performance of the battery for reuse/ recycle purposes; a process which has an expense associated with it due to transportation, testing equipment, materials and staff costs.

A key outcome from this proof of concept was to understand what is involved in China Unicom delivering a commercial service to customers in providing distributed ledger solutions. The remainder of this document attempts to identify the opportunities and benefits to mobile operators and their customers in delivering distributed ledger products and services.

[7] Understood to include passenger cars and buses

3 DISTRIBUTED LEDGER NETWORK ARCHITECTURE

A total of seven interconnected nodes were provided for the distributed ledger proof of concept, as shown below (Figure 1), by China Unicom, Wanxiang Blockchain Company and Wanxiang Institute:

China Unicom (labelled CU), providing two nodes

Wanxiang Blockchain Company (labelled WBC), providing one node

Wanxiang Institute (labelled WXRI), providing four nodes

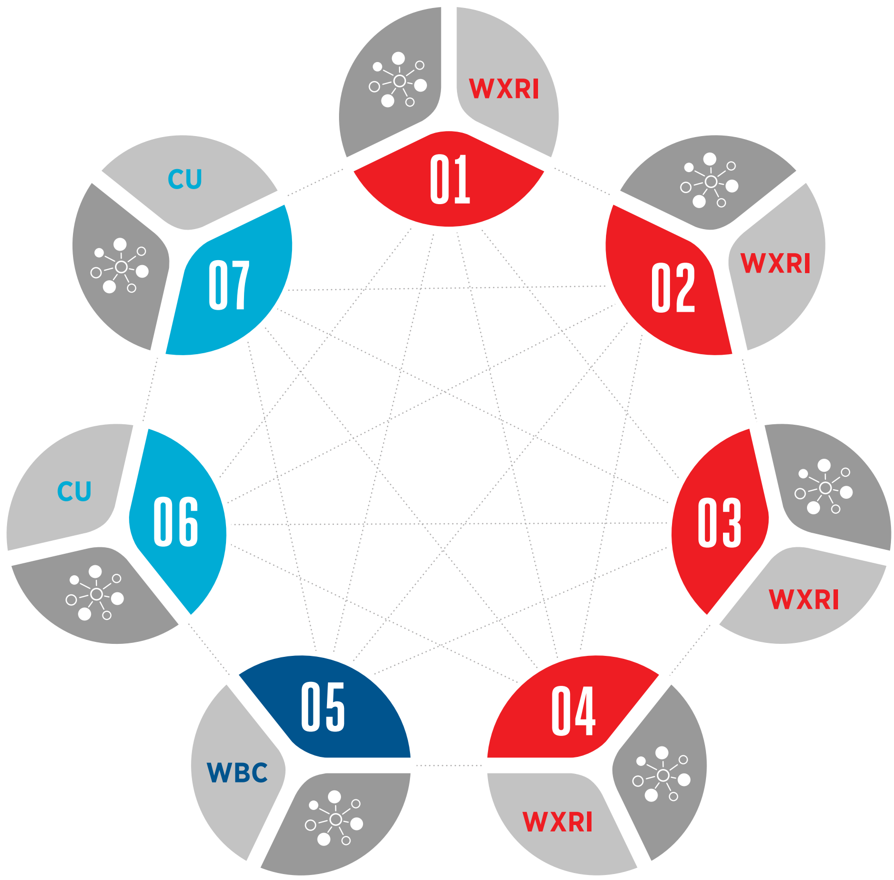

Figure 1. High level network architecture

For this proof of concept Wanxiang Institute provided the business applications working with the distributed ledger. The two other parties provided nodes to validate and witness the information on the ledger as shown in Figure 2.

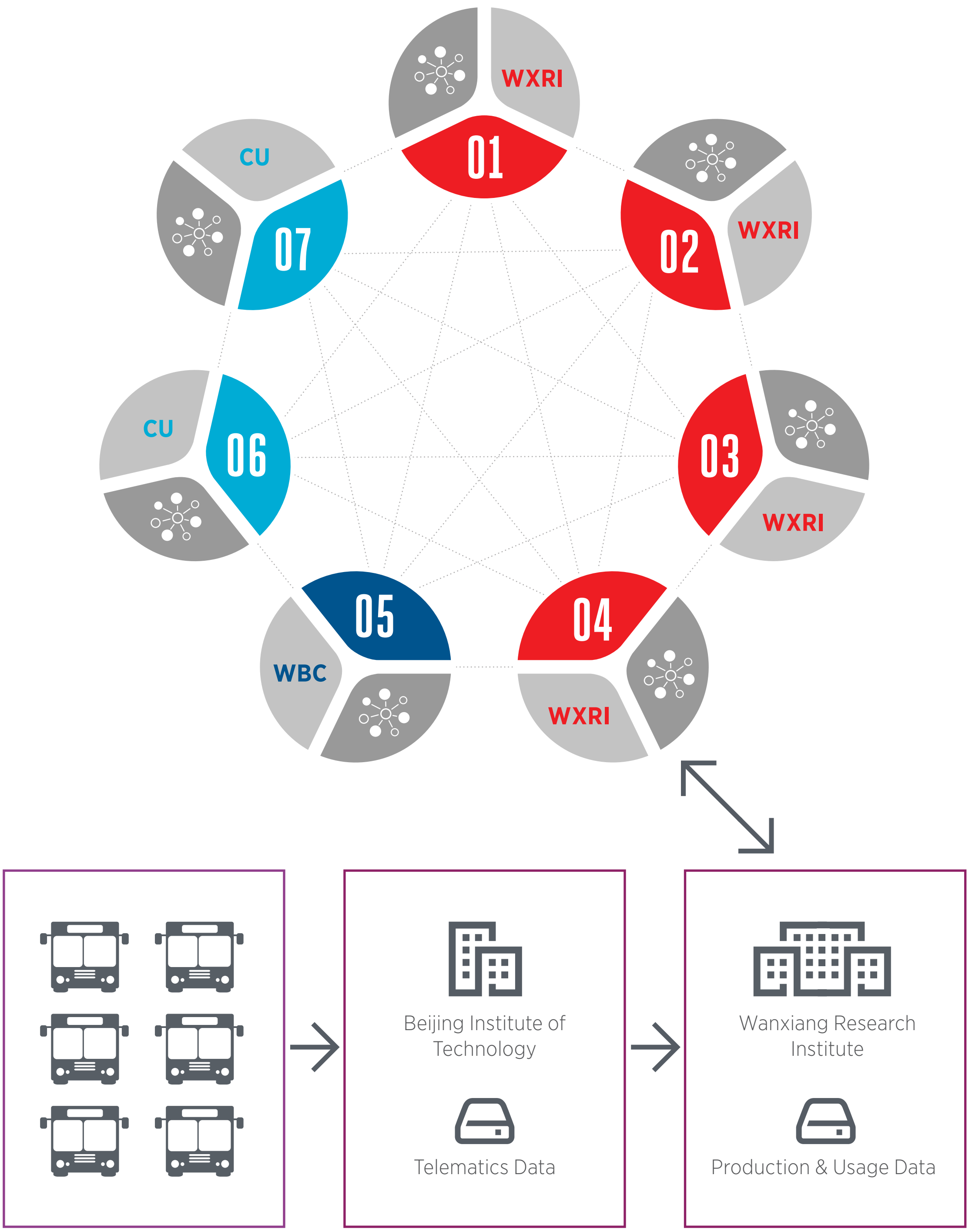

Figure 2. Flows of information to/from the distributed ledger network

An important consideration in this deployment was what information would be stored on the distributed ledger.

- The information on the distributed ledger is replicated to all nodes, which means that all parties have access to the same information. This could be an issue if unencrypted confidential information, which should not be shared with all consortium members, is stored to the distributed ledger;
- Distributed ledgers are immutable[8] and therefore compliance with privacy regulations, such as requiring the ability to delete personal information, or limiting the storage time of other business information, necessitates the use of complementary techniques such as 'off-chain storage'.

'Hashes'[9] of the battery information were generated when the original data was acquired and these hashes, rather than the original data, were stored on the distributed ledger. The initial value and charge cycles information on battery modules is commercially confidential to the Wanxiang Institute. Therefore it was decided to keep the confidential battery information within the internal IT systems of Wanxiang Institute and distribute only copies of data hashes to the distributed ledger. This provided a way for authenticating the accuracy of the battery records stored on the IT systems of Wanxiang Institute because it is practically impossible to alter these records without changing the original hash value. This provides an excellent operating model for more general distributed ledger deployments.

In this way, Wanxiang Institute can rely on the distributed ledger to add confidence to the authenticity of the battery charging records it is holding in its internal systems. The inherent immutability of the ledger as well as the strong cryptographic techniques used in the ledger and in hashing functions provide authoritative provenance concerning the party storing entries in the distributed ledger, and also the ledger is replicated across multiple parties for increased integrity and assurance.

Since the parties forming the distributed ledger consortium include organisations with the credibility of a mobile network operator such as China Unicom, this provides a further stamp of authority around the fact there has been no tampering with the battery charge and related information. Therefore, these various attributes of the distributed ledger are providing trustworthiness and truthfulness useful and valuable to businesses in their dealings with external parties. Wanxiang Institute can then use the distributed ledger to prove the truthfulness of internal records on battery value and usage so that at the end of the useful life in an electric vehicle the best reuse/recycling choice can be made and the second hand value of battery modules can be maximised.

[8] It is possible to append information to a distributed ledger but not delete any information previously store

[9] A 'hash' is an 'irreversible' computational function that generates a value from input data. Provided the hashing function is sufficiently complex, and the resulting number of bits of output data is significantly less than the number of bits of input data the hash function can be used to protect the confidentiality of input data whilst still making it possible for a third party to authenticate that data.

4. COMPARISON BETWEEN DISTRIBUTED LEDGER AND 'LEGACY' SOLUTIONS FOR PROVING AUTHENTICITY

It is useful to compare distributed ledger solutions with a 'build your own' solution which is able to provide equivalent authenticity proof for data, particularly in the case such proof is required between different organisations which work together. Essentially, distributed ledger solutions combine a series of existing technologies, tools and processes. Many of the technologies and tools used in distributed ledgers are 'off-the-shelf' or open-source. For example, a distributed ledger 'stack' typically integrates the following:

An off-the-shelf database used to store the ledger transactions

A set of API services that allows transactions to be read and appended

'Standard' cryptographic processes and signatures implemented by off-the shelf libraries

Peer to peer synchronisation

Consensus algorithms

The ability to execute code in the form of smart contracts

What are the desirable attributes in an equivalent 'build your own' solution[10] providing strong information provenance between multiple organisations?

- Multiple individuals or organisations must be able to collaborate on the platform to store and/or verify information;
- It is possible to demonstrate that records stored in a database have not been tampered with since they were stored;
- It is possible to unambiguously prove which user or system stored the record;
- The solution must be robust against malevolent actors;
- The solution must be able to continue operating even if one member organisation suffers a system outage.

How then are off-the-shelf distributed ledger solutions different from a 'legacy' or 'build your own' solution delivering the above functionality by combining a set of the above listed off-the shelf products along with customised code?

10 Note that databases (such as Oracle) provide audit tracking, but these are typically used deep within the IT systems of a single organisation to track actions, they do not easily extend to external organisations.

CONSIDERATION	DISTRIBUTED LEDGER	'LEGACY'
'Productisation'	The distributed ledger platform developers have done all the work in choosing the various components to use, developing integration 'glue' and any customised code, testing all components, and making it easy to install with supporting documentation. Saves customers time & effort and avoids the need for specialist expertise Development is done once and then reused across implementations	All the same work needs to be done by the service provider which will lead to a significant amount of technical work and time. Requires specialist expertise to select & integrate components leading to high costs and time to market Development (and learning) is done each time by each service provider
Adaptation	Commonly, distributed ledger platforms are released on an 'open source' basis allowing for easier adaptation of the solution. Adaptation is possible, which may be easy for simple changes There will be some constraints based on the ledger design	As a fully bespoke solution it is possible to develop exactly the functionality required – but this is likely to involve a larger effort and require more time than using an 'off the shelf' integrated ledger solution. Much more customisation of the solution is possible. Development and customisation will be significantly costlier and take much longer
Roadmap	Developers will evolve the ledger platform with new features, and ensure maintenance (patching) for updated versions of system dependencies. The roadmap will be decided by the ledger developer community. Many new features including security enhancements will be provided 'automatically' and 'for free' Roadmap for the core platform is however essentially dependent on the platform developers	Any developments can be decided by the integrator or solution provider, though they will also have to support and maintain the code and perform patching for any related system dependencies. Much more ability to decide and implement the roadmap Much more effort required to maintain and enhance the platform and therefore at much higher cost than an 'off-the-shelf' ledger

CONSIDERATION	DISTRIBUTED LEDGER	'LEGACY'
Engineering cost	Generally the development cost will be amortised over a large number of clients and/or funded by other means (e.g. token sales). Ledger implementation can be achieved at very little cost	All platform selection work, integration, test and maintenance will fall on the integrator. Even basic platform implementation will bear a significant cost, as well as ongoing maintenance costs
Time to deploy	Often can be achieved in hours or days. Ideal for rapid deployment, even with a functionally rich solution	Likely to take several weeks to several months to select and 'bolt' the various components together. Slow to implement even a basic solution
APIs for system integration	Usually comes with a set of APIs designed to support ledger operations from client systems. APIs have already been built to support standard use cases Dependency on ledger designers to have good API designs suitable for required use cases	These will need designing and developing, whilst not a difficult task there is an amount of experience required in good scalable & secure API design. Optimised APIs can be designed to support required use cases API design expertise may not be available, additional time/effort to design, and increased risk of poor design (especially regarding security)
Platform independence	Usually the distributed ledger platforms are not tied into a particular hardware/software platform. They will usually run on 'commodity' systems hardware and on Linux platforms (or using containers) giving a high degree of choice. General platform portability avoids costly lock-in to specific platforms	Development staff will usually choose platforms they already know, this is more likely to lead to a risk of software and/or hardware lock-in. Lock-in can be avoided but might make the development more expensive and lengthier. Operationally good for organisations as platforms are the same as other systems Potential for higher running costs due to lock-in to specific (costlier) operating environments

CONSIDERATION	DISTRIBUTED LEDGER	'LEGACY'
Usage charges (transaction costs)	For those distributed ledgers which have 'access fees'[11] for processing transactions, there can be a disincentive against usage particularly for lower value transactions[12]. 👍 Initially (at small scale) the fee structures can be very attractive 👎 At large scale the fee structures can be expensive	The various system resources provided for the distributed ledger will have a generally fixed cost irrespective of the number of transactions being processed. 👍 Costs are likely to scale better at high volumes (system costs amortised over a larger number of applications/ users) 👎 At lower usage the fixed system costs can be significant making each transaction comparatively expensive
Functionality	Whilst there are many distributed ledger platforms these may not have exactly the functionality required for a given application. Issues such as data privacy and data localisation may or may not be addressed as required. 👍 There are many existing platforms 👎 Time and effort (& therefore cost) to identify & validate fitness for purpose	As a 'build your own' solution it's possible to develop exactly the functionality that is required for the application. This can include key topics such as data privacy and localisation as required by country or regional regulations. 👍 Exactly the required functionality can be built 👎 Time and effort (& therefore cost) to build an equivalent solution will be significant
Skills & knowledge	Distributed ledger solutions are developed by teams who have acquired or built the relevant skills & knowledge across all the required components. Often this is over a period of months or years. 👍 Little need to acquire or develop skills & knowledge in-house for the distributed ledger platform	Companies building solutions using legacy approaches will need to acquire sufficient skills & experience to suit their needs. This inevitably takes time and may be difficult. 👎 Requires a larger development team also on an ongoing basis, much more expensive, longer to build team

[11] Usually for public distributed ledgers which have some form of token used to pay for service e.g. Ethereum, IOTA
[12] Some crypto currency tokens can have quite high transaction charges

CONSIDERATION	DISTRIBUTED LEDGER	'LEGACY'
Commercial longevity	Some distributed ledger developments are based on speculative projects, and therefore it's important to understand there can be a risk to business/project continuity. Open source can mitigate this risk (in part), but that would require resource for continuity Risk of continuity must be evaluated, and it will not always be clear who is behind a project and what the funding continuity will be	With a legacy solution it is possible to base this on components with a high confidence of ongoing support and development. More ability to select components with assured continuity Requires additional work on behalf of the solution integrator to choose and integrate required components with a consequential and potentially significant increase in project cost

In summary, a distributed ledger platform offers the advantage of it being essentially ready to use immediately. This will generally mean lower project startup time and costs, and a much reduced need for engineering and related technical skills for the core platform. It ensures there is no need to 'reinvent the wheel' for the functionality provided by the distributed ledger platform.

An equivalent solution based on legacy products can be built with potential advantages in providing more targeted functionality. However, this will have a much longer project implementation time, a substantially greater engineering and maintenance cost, and require the hiring of specialists who can deliver the necessary functionality.

5. OUTCOME AND FINDINGS FROM THE PROOF OF CONCEPT

China Unicom and Wanxiang Institute demonstrated a working proof of concept for the battery tracking use case at MWC Shanghai between the 26th and 28th June 2019.

Figure 3. China Unicom and GSMA presenting the Distributed Ledger solution at MWC Shanghai

Figure 4. China Unicom, GSMA, Wanxiang Research Institute and Wanxiang Blockchain Company kick-off meeting in Shanghai

The business application, developed by Wanxiang Institute and China Unicom, was a web application which showed battery information including battery-charge times, battery-discharge times, attribute information of batteries, and so on. This connected with the distributed ledger network which stored the corresponding information hashes.

The proof of concept demonstrated the possibility for a multi-organisation distributed ledger consortium to be delivered within a short space of time (in a couple of months) and with computer systems operating in different hosting environments.

A number of useful learnings were gained along the way:

LEARNING	IMPLICATION
Distributed ledgers follow a 'federated' model often described as a 'consortium'. Membership administration is a very important role. This administration function is responsible for controlling which organisations and nodes are members of the distributed ledger consortium.	A trusted party needs to be nominated for the role of 'membership administrator'. It is an ideal role for a mobile network operator to fulfil in delivering a distributed ledger service on behalf of enterprise customers.
'Private' distributed ledger solutions are better for securing the privacy and confidentiality of data compared with public blockchains.	Public blockchains can be useful for proof of concept development, but usually will not deliver required privacy and confidentiality features. Therefore a consortium/federation of partners needs to be formed to establish a private network. Mobile operators can have a key role to play in providing blockchain nodes, membership administration, and solution design.
Installing the distributed ledger software is normally relatively quick[13] (less than one day's work), but there are many other tasks involved in 'productising' this into a commercial ledger node, particularly from an IT security and operations perspective. Key needs include - Security, including "hardening" of nodes; - Firewall settings; - Node monitoring; - Operating system & platform patching; - Organising backups.	IT security and operations are key components of an enterprise grade distributed ledger service, and one that is in a sweet spot for mobile network operators because these are regular operational activities in delivering the mobile network.
The information to be recorded on the distributed ledger needs full consideration both regarding personal data and commercially sensitive data.	Blockchain solutions which provide a combination of on-chain (immutable) storage and off-chain (amendable) storage are more useful for business applications.

[13] This is of course dependent on the platform chosen

LEARNING	IMPLICATION
Node participation in consensus was found to depend substantially on the performance of the networking connection between nodes. This was found to be more important than other system resources, e.g. memory and CPU performance.	Mobile networks contain high performance networking backbones supporting high availability nationwide networks, this provides a strategic advantage for enterprise distributed ledger networks as the mobile network can deliver high performance private networking to maintain distributed ledger consistency and consensus.
The distributed ledger platform is an important, but relatively small part, of an overall business solution. It is essential that connectivity is provided (via network APIs/ SDKs) for business systems to integrate with the distributed ledger.	Enterprises will need support, tools, and documentation and on-going management if they are to successfully use distributed ledger solutions in their applications.
It was found the distributed ledger stack produced a substantial quantity of synchronisation logging information – enough to fill up the hard disk, so requiring the purging of excess logs.	Further tools and operations management are necessary when moving from a test installation to a production environment.

6. OPERATOR ROLES AND REVENUE OPPORTUNITIES

Based on the observations and learnings from this proof of concept, the following roles for operators and revenue opportunities have been identified:

ROLE SUMMARY	DESCRIPTION/ REVENUE OPPORTUNITY
Simple hosting provider / edge provider	The MNO provides simple hosting services which allow ledger nodes to be deployed by a customer. This is suitable for customers with their own IT operations teams and replaces the use of conventional hosting/cloud providers. This can be 'simple' hosting ('bare metal') allowing the customer to install and configure the operating system through to the distributed ledger software. Alternatively, it can be in the form of virtual machines or containerisation services which allow the customer to deploy the distributed ledger software. Edge computing can be used to provide hosting infrastructure, with the advantage of reduced latency between devices and the distributed ledger network. Revenue opportunities for this role would be based on conventional hosting type fees (monthly/ annual) based on the resource capacity leased, e.g. number/speed of CPUs, memory size, storage space and network connection speed.
Peer node provider	In this role, the operator would provide the distributed ledger software installed and configured as one or more nodes which are part of a consortium network administered by another party. This provides resilience to the consortium network, using the systems and processes of the operator to meet required SLAs. The operator as the provider of nodes also adds their credibility to the operation of the consortium network, so that third parties have a higher confidence in the integrity of the information stored on the distributed ledger. Revenue opportunities for this role would be based on a per-node price with a typical monthly/annual basic lease price. The pricing could also include variable fees based on the number of transactions handled/accumulated in the distributed ledger. Typical also would be price banding according to the required SLA.

ROLE SUMMARY	DESCRIPTION/ REVENUE OPPORTUNITY
Network administrator (& node provider)	The operator delivers one (or more likely) more nodes which form part of a consortium distributed ledger. In addition, the operator takes on responsibility for administering membership of the network on behalf of the consortium or enterprise. This is useful for customers which want to incorporate distributed ledger technology into their own solutions, but do not have the expertise, processes or available resource to administer the distributed ledger network. It is expected the consortium or enterprise would deploy at least one or more nodes. The revenue opportunities for this role would include a higher service component on top of usual hosting fees. This could include an additional monthly or annual management fee, dependent on the service level required by the consortium/enterprise.
Full network provider	In this role, the mobile network operator is delivering a complete distributed ledger network as a service. This includes all (or a majority of) nodes, administration, and related support. This is useful for a consortium or enterprise that wishes to use distributed ledger technologies but does not want to provide nodes or be responsible for administering the network. Operators can leverage strategic assets in edge computing to provide low latency ledger services and/or geographical localisation of data for example to a business or educational campus. The revenue opportunities for this role would reflect the full service offered in delivering a distributed ledger ‘as a service’, with the potential for premium charging for high SLAs.
Professional services provider	Mobile operators can also offer bespoke professional services, either technical or business, related to distributed ledger adoption or implementation. This can leverage technical or business expertise built by the operator from their own distributed ledger implementation projects. These services can complement any of the previous options, or could be totally bespoke and standalone for enterprises or business consortia interested in using distributed ledger solutions. It is attractive to enterprises or consortia to ‘buy in’ such expertise as it can be difficult to hire teams quickly, for sometimes short assignments, with the required expertise. In the professional services market revenues are usually based either on a project basis or on a time & materials basis. Usually, there can be a significant margin added to direct staff costs, typical in IT or business consulting. Operators could be competing with IT or management consultancies, the same could also be delivery partners.

7. CONCLUSIONS

Distributed ledger technology platforms are now sufficiently mature that they can be incorporated into product and service offerings. However, simply deploying a distributed ledger software stack is only a small part of delivering a complete product or service. In particular, there are key issues in operations, support, customisation and solution design that must also be addressed.

Mobile network operators have proven experience in turning specific technical solutions into complete products and services, particularly, of course, in respect of delivering a range of innovative mobile network services. It is expected the capabilities and resources of mobile network operators can similarly be applied to 'productising' distributed ledger platforms, as seen in part in the China Unicom proof of concept.

The position of mobile network operators in the distributed ledger eco-system is also valuable. Mobile network operators can offer a key role as authoritative members or suppliers of distributed ledger solutions, offering enterprise customers a higher degree of trust for the distributed ledger networks they could otherwise deploy. Thus, even for those organisations which are technically able to deploy their own distributed ledger solution, there is still an important role that mobile operators can fulfil.

Therefore, although realistically it is still early in the adoption cycle of distributed ledger technologies for the IoT, it is clear there are a variety of roles for operators to play in delivering distributed ledger based solutions. It is important to note that operators can, as demonstrated by China Unicom, convene partnerships with technology and resource providers in order to deliver these roles, with the mobile network operator leveraging their organisational credibility and operational excellence to provide customers with commercially attractive distributed ledger solutions.

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators and nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: @GSMA.

For more information please visit:
www.gsma.com/IoT

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601